Barsky, Simon

From: Goeckner, Gregory
Sent: Monday, January 24, 2000 7:12 PM
To: Barsky, Simon; Litvack, Mark; Cohen, Tod; Attaway, Fritz; Robbins, Dan
Subject: FW: WAEA DVDWG Key Mgmt. Strawman

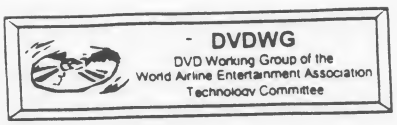
DVD0001_Key_Mgmt.pdf FYI. As you know, Schumann submitted an important affidavit in the DeCSS case in New York. I thought you would be interested in what else he is doing for the member companies.

-----Original Message-----
From: Hanniball, Wade [mailto:wade.hanniball@umusic.com]
Sent: Monday, January 24, 2000 7:04 PM
Subject: WAEA DVDWG Key Mgmt. Strawman

Attached is proposed strawman language on key management authorities offered by Robert Schumann, Cinea LLC (in fulfillment of his homework assignment from our last meeting). This document will be discussed at our meeting Feb. 1-3 at the Burbank Hilton.. Thank you, Rob, for your contribution.

--
Wade Hanniball, DVDWG Co-Chair
Universal Studios
818-777-5194 tel.
818-866-0995 fax
wade.hanniball@umusic.com

<<DVD0001_Key_Mgmt.pdf>>



DVDWG Document 00/01

Subject: Strawman WAEA Early Window Key Management Authority Functions

From: Robert Schumann, Cinea LLP

Date: January 20, 2000

Proposed addition to section 11.4 on Key Management:

The primary function of a key management authority (KMA) is to provide assurance that content is enabled only for authorized playback devices and that all private keys used in the system remain confidential. The functions described may be performed by one or more KMAs, each of whom may perform all or part of the indicated functions. In cases where the KMA functions are shared among multiple KMAs, they shall cooperate in a secure fashion under content provider direction.

A Key Management Authority shall:

- Securely create, store, assign and monitor the Key-Loading Key for each authorized security module.
- Securely create, store, assign to security modules, monitor, and revoke the Device Keys.
- Support Device Key updates as necessary.
- Generate encrypted Content Key Tables for content based on a content provider s (or its KMA s) authorized player list.
- Securely create, store, assign and monitor Content Keys.

A Key Management Authority shall document its policies and procedures for:

- Playback device activation, authorization and authentication, including handling of Key Loading Keys and Device Keys.
- Performing Device Key updates.
- Creating Content Keys.
- Generating a Content Key Table.
- Creating, managing and implementing device key revocation lists.
- Interacting with other KMAs.